ORIGINAL

UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:	)	GN 09-51
	)	+
700 MHZ NATIONWIDE INTEROPERABLE	)	PS 06-229
PUBLIC SAFETY WIRELESS BROADBAND	)	
NETWORK WORKSHOP	)	

Pages: 1 through 94

Place: Washington, D.C.

Date: March 17, 2010

HERITAGE REPORTING CORPORATION

Official Reporters

1220 L Street, N.W., Suite 600

Washington, D.C. 20005-4018

(202) 628-4888

contracts@hrccourtreporters.com

IN THE FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF:)
)
700 MHZ NATIONWIDE INTEROPERABLE)
PUBLIC SAFETY WIRELESS BROADBAND)
NETWORK WORKSHOP)

Commission Meeting Room
FCC Building
445 12th Street, S.W.
Washington, D.C.

Wednesday,
March 17, 2010

The parties met, pursuant to the notice, at 9:32 a.m.

BEFORE: JULIUS KNAPP, Chief, Office of Engineering and Technology, FCC

ATTENDEES:

JAMES ARDEN BARNETT, Jr., Chief, Public Safety and Homeland Security Bureau
STAGG NEWMAN, Chief Technologist, National Broadband Team
JOHN PEHA, Chief Technologist, FCC
JENNIFER MANNER, Deputy Bureau Chief, Public Safety and Homeland Security Bureau
WALTER JOHNSTON, Chief, EMC Analysis Division, Office of Engineering and Technology

APPEARANCES: (Cont'd)

Presenters:

ALLAN SADOWSKI, Information Technology Manager, North Carolina State Highway Patrol

ROBERT LeGRANDE, II, Former Chief Technology Officer, District of Columbia Government, President and Chief Executive Officer, LeGrande Technical and Social Services, LLC

PATRICK RINGQVIST, Vice President, Wireless Network Solutions, Ericsson, Inc.

ROGER QUAYLE, Chief Technology Officer and co-founder, IPWireless, Inc.

MARK McDIARMID, Director, RF/RAN Systems Engineering, T-Mobile USA

DALE N. HATFIELD, Executive Director, Silicon Flatirons Center, University of Colorado at Boulder

P R O C E E D I N G S

(9:32 a.m.)

MS. MANNER: Good morning, everyone, welcome to the 700 MHZ Nationwide Broadband Public Safety Wireless Network Technical Forum. What I'd like to do is welcome you this morning, welcome our panelists, and introduce Jamie Barnett, the Chief of the Public Safety and Homeland Security Bureau.

MR. BARNETT: Jennifer, thank you, and thanks to all who have made this possible. Thank you for being here, and especially to our panelists today. Just a couple remarks before we start. We were excited about having this, the panel, since really there has not been much going on here at the Commission for the last few weeks and months and we needed some excitement.

Actually, with the delivery of the broadband plan yesterday, while that may be a culminations in some ways it's actually also a beginning, and we are excited about it, you've seen the amount of comments that are coming in, there's a lot of excitement about it. One of the ones that I'd like to highlight to you, and they're coming in from the Congress as well, but the President himself made comment.

And I'll actually quote him here, "My

Administration will build upon our efforts over the past year to make America's nationwide broadband infrastructure the world's most powerful platform for economic growth and prosperity, including improving access to mobile broadband, maximizing technology innovation, and supporting a nationwide interoperable public safety wireless broadband network."

It's good to have the President, Commander in Chief, recognize that and say that he supports that, and gives me great hope for moving forward. With that, I'd also like to make announcement this morning, because the broadband plan also maps out a great deal of work for the FCC. Today as one of our very first actions following the release of the National Broadband Plan, we'll be issuing a public notice seeking comment on the NPSTC Broadband Task Force recommendations as submitted to the Commission by the Public Safety Spectrum Trust.

We'll be seeking input concerning these recommendations that address the technical aspects of interoperability of state, local, and regional deployments that are the subject of pending waiver requests. Our intent is to determine the extent to which these recommendations could form the basis for action on these waiver requests, including technical

and operational requirements for the Emergency Response Interoperability Center and what it would adopt.

The comments date for the interested parties is April 6, I believe, and then the deadline for reply comments is April 16th. Following the receipt of comments, we'll move quickly to act by early to mid summer on the waiver requests to that those agencies seeking to deploy public safety broadband networks will have the initial set of requirements necessary to pursue any desired partnerships in network deployments.

At the same time, I'm glad to see that NIST and NTIA through their Public Safety Communications Research Program are seeking participation in a demonstration network for the public safety broadband communications in the 700 MHZ band. We believe that this demo network would complement the FCC's overall efforts for ensuring that first responders have access to a nationwide wireless interoperable broadband public safety network, and including action on these waiver requests.

So some of you have heard me say this before, but I certainly want to emphasize it now. When we took this on, there were a few requirements

that I asked the team to look at. Number one, it was going to be fact driven, data driven from the very beginning, we would base our decisions on that, and we would look at everything. And so at one point we had some 27 options on the table that got narrowed down to what we think is the best plan to move forward.

What I told them is, the plan is going to have to be truly nationwide, it has to extend from the densest city down to the most rural area in America. It has to be truly interoperable, that is the overall goal that we have to have. And it has to be viable, both from the economic standpoint that companies would want to partner with public safety agencies, public safety agencies would be able to afford this, but also that it would be viable from a technical standpoint, which brings us to today.

Now, there has been a lot of debate and obviously a lot of concern about the D block, and you'll get to hear about that and ask questions about it as well. One thing that I think is interesting -- and I got to see all of the presentations that you'll see today -- one of the things that I would emphasize are the areas of what I would call growing agreement on.

So I mean I think everybody agrees that we

need to have a nationwide and interoperable network, but I think you'll see there are some other areas of agreement, such as that we need funding for this, because truly it will not be nationwide and it probably won't be interoperable unless we have some public funding for this. And the plan puts forth some very I think innovative ideas about moving for that. We have to have funding, we have to start talking about that we need funding, and you'll see that today.

There are also some areas which you might say of concern that I think you'll hear about today, and that's the roaming and priority access. I have that concern too. That's why the plan actually maps out that we are going to have a very intense program of making sure that we get priority access and roaming right, and so that's fair game today and we want to talk about it. Once again, thank you for being here, thank you, panelists. And I'd like to turn it over now to our Chief of the Office of Engineering Technology, the one and only Juli Knapp.

MR. KNAPP: Thank you, Admiral Barnett. Welcome, and happy St. Patrick's day to all of you. In keeping with St. Patrick's day we are hoping today to have a robust discussion followed later on in the day by a robust celebration. Yesterday was truly

exciting for the Commission in rolling out the National Broadband Plan. The public safety piece of that is one of the most important and vital parts of the plan.

And for the engineers, as exciting as yesterday was, today when we get down and start talking about the nitty gritty details of the technology, that's what really turns on the engineers. So we're going to kick off the day with a presentation by Dr. Stagg Newman, who is our Chief Technologist in the National Broadband Team, and Dr. John Peha, who is Chief Technologist of the FCC. John and Stagg?

MR. NEWMAN: Thanks, Juli. I've got the easy part, I do the first two charts and then hand over the technical work to John. Maybe in keeping with the theme of St. Paddy's day, one of the challenges that we had to answer from Admiral Barnett was the green challenge. And in this case, green means making it affordable, green as in the color of money as opposed to the energy green.

So what we've tried to do is come up with a plan that we think cost effectively uses the commercial assets our there but give public safety their own spectrum for their core use and takes advantage of all the different ways to meet their

needs. If you look at the requirements, you know, high performance uplinks, high capacity, performance inside buildings, and performance in wilderness areas and remote areas, there is no way you can build a single network architecture to meet that unless you can afford to put out literally, if you tried to meet all those requirements with a single network build, hundreds of thousands of cell sites and you'd have to go to Congress $50 billion, $100 billion.

That's not going to happen unfortunately in this environment. So we've tried to look at all the things that go into a network architecture. If we could flip to the next slide please? Thanks. And say, how do we come up with a total plan to meet public safety's needs? So we came up with what we are calling the pyramid chart. Light up the public safety broadband spectrum, 10 MHZ. Give them their own radio access network but use commercial assets, and give public safety on a local basis the choice to choose a partner.

They may choose a current cellular wireless operator, they may choose a new D block operator, a new systems integrator, that's their choice, but use the commercial sites that are out there, the back haul that's out there, leverage off all that. Okay, so

that's the core day to day public safety broadband network using 700, which has, you know, great propagation characteristics. Now, there will always be times when you don't have enough capacity. I don't care whether you have 10 MHZ, 20 MHZ, if you truly have a Pentagon type disaster or a Katrina type disaster, you need more capacity.

So for those true dire emergencies, do a priority wireless broadband service. You'll hear a lot more from John about how that works, but the good news is in a modern IP world, you can have the type preemption priority et cetera you need so public safety truly gets the priority they need. The 911, you know, consumer calls can still go through, but, you know, people aren't doing video games in a dire emergency. You know, same technology that's used in the military to make sure for example admirals have priorities over generals in an emergency. Moving on.

(Laughter.)

MR. NEWMAN: Okay, but we've got another problem, how do you get deep inside buildings? You know, large commercial buildings where either you may have very high populations in an emergency and certainly you can't get a signal that's from an outside distant antenna deep inside buildings, as we

all know if we try to use our cell phones as we go up an elevator. So there we really need in-building systems, distributed antenna systems or pico cells that will light up the public safety spectrum, you know, not just the commercial spectrum but the public safety spectrum.

So that's a continued push on the building codes and other requirements to make sure on a going forward basis commercial buildings of reasonable size will have indoor systems. And then finally, there will be times where you don't have a cell system where you need it, okay, either because a natural disaster, a tornado's come through, a hurricane, or because the disaster's out in the wilderness area, a train's gone off, you know, the tracks with a chemical spill.

So let's have a fleet of deployables. And again, the good thing in a modern LTE architecture is the deployables are going to be much less expensive, much lighter. Also, particularly in remote America, people get out to the emergencies by vehicles. Turn those vehicles into relay systems. So that's our total plan. The plan focuses -- could we have that, back one please, yeah. The CAPEX funding focuses on the bottom and the top of the pyramid, the middle parts will be addressed through requirements and also

through the operators being able to achieve a return of fair and reasonable rate, and we'll go into the details of that plan in more detail.

Now we're ready for the second chart. Just going to highlight the cost today, we've had details meetings with public safety going through the cost model in detail, and we've verified that with a lot of operators and equipment manufacturers, so we're pretty confident that our costs are good numbers that we've put into the request to Congress. $6.5 billion CAPEX, and an ongoing OPEX that will grow to about $1.2, $1.3 billion in year 10.

On the CAPEX, we again, to be pragmatic, we said, okay, to serve 95 percent of Americans, okay, 95 percent of the POPs in America will have LTE by commercial forces within the next five years, based on announcements of vendors, what's going to happen in the commercial market. In fact, the announcements are actually more ambitious than that, but we said they'll miss their dates by a year or two but not by more than that.

So 95 percent of America will be served by LTE, that means the cell site architecture, the back haul architecture and all will be driven out there by commercial market forces, let's capitalize on that.

We estimated that it takes a little over 40,000, 41,000 cell sites will be needed to serve that commercial architecture and light up the cells that you have to light up for public safety. Again, we think that's conservative, you could probably do it more like 35,000 but we said, let's do it with 41,000.

A little under $100,000 per cell site, $95,000, multiply that out, so that's $4 billion to light up the commercial, take the commercial assets, allow public safety to partner with whomever they choose through an RFP process, to light up their spectrum. So now with $4 billion furnished, we hope, through the appropriations process from the Federal government, public safety now has their spectrum lit up nationwide.

We also said we'd like those sites hardened, structurally hardened, battery backup, et cetera. So we put in $1.5 billion for that. Then we said, we still have to serve rural America -- oh, I should say, and that's to serve handhelds, because that's what that is going to be built out to. In fact public safety will have better service than the average consumer you or I because they'll have handhelds but presumably they don't care as much about form factor and coolness, better batteries and a little, you know,

antenna on top, they're going to have better performance and better coverage than the consumer if we get the right device ecosystem, and we'll talk about that later.

And then, we've got to serve rural America. Okay, rural America we said it's not pragmatic to build out the handhelds to cover vast amounts of rural America, but we do want to get from 95 to 99 percent of the population, so we said we'll build a network for vehicular coverage. So you're now hitting, you know, antennas on vehicles high gain devices, we think you can do that with a little over 3,000 towers -- again we estimate that in many different ways.

And so we'll build out that, put in $800 million to build out in rural America because those sites, we won't have an LTE infrastructure, so we may have to use 2G sites, we may have to use LMR sites from public safety. We thought, three quarters of the cases we can find a site but we've got to build a whole 4G infrastructure on that site, quarter of the cases we may not even have a site out there, so there we put in money to build new towers.

So that $800 million gets you the buildout to 99 percent of America. The program did not include funding for the devices, but by using LTE

infrastructure and the components and guts of commercial devices, we think the device costs can be driven down from several thousand dollars today to the several hundreds of dollars, so that's a tremendous improvement in the budgets for public safety.

OPEX -- and then, oh, I'm sorry, we also put in $200 million for this fleet of deployables and for equipping vehicles in rural areas as relay stations. OPEX, our model is there would be a fee on broadband consumers' bills, the same way we pay a fee for 911 today, not very large, you know, less than a dollar per month, and that would fund the ongoing OPEX growing to $1.2 or 3 billion in year 10.

That would allow public safety to pay whoever their commercial partners are, operators or systems integrators, to operate that RAN infrastructure that's up on the tower, okay, the antennas and electronic processing and all that takes care of their spectrum, pay to transport their bandwidth, their bits or packets, back to the public safety agencies through a standard IP network in a secure private way the way it's done for the military and other mission critical enterprises.

Additional costs were thrown in for rural America because you always have additional costs in

that environment. We did say when they have to use the commercial network for priority access, as the Chairman said in his speech, that would be through commercial agreements but at a most favorable nation type of approach. So that's our basic approach to cost. I'll turn it over to John for technical details. Thank you.

MR. PEHA: So that was two slides. I think I'll be moving a little faster through the other eleven, but you have the slides, I believe, if you want to see the details. So I think we have a very both effective and cost effective strategy here with a lot of elements to it that sort of build on each other. Just to run through at a high level what some of those elements are and then I'll drill down a little on a few of them.

We envision authorized network operators deploying and operating a broadband network designed specifically for public safety and public safety's unique needs in 10 MHZ of spectrum. In some regions we expect this to be an incentive based partnership with a commercial entity, and I'll talk more about that in a minute. Others may already have their own infrastructure which they can use as well.

Another important element of this is, as

Stagg has already commented on, is public safety's ability to use commercial networks in their area by roaming and on a priority basis. Again I'll also comment more about that. Another very important element, as Jamie Barnett has discussed, is funding for network construction, operation, and evolution. We have grants for capital expenditures and the broadband fee for operational.

This makes a nationwide buildout of infrastructure possible, including rural America, and also where infrastructure exists it can help harden it to meet public safety requirements. Fourth important element, requirements that will lead to the creation of devices that serve public safety and operate in public safety spectrum. And finally, to make sure that this is interoperable that there are standards across regions, an Emergency Response Interoperability Center.

So we envision this as a network that will support diverse services and divers application, data and voice services over an IP based transport system from the beginning, forming what is initially perhaps a more reliable version of sort of cutting edge commercial offerings, and then evolving to support mission critical voice and video and data as well.

And we see at least 256 kilobits per second per device even at cell edge to support things like video.

So priority is a piece of this. Priority, or rather, priority access and roaming, public safety users would be able to roam onto up to 70 MHZ of spectrum that is licensed to commercial systems. This obviously gives them access to a great deal more capacity. Maybe less obvious but it is also important for dependability. If the hurricane takes out the public safety cell tower which is closest to you, hopefully some other tower is still functioning that you can use. And similarly, having multiple networks improves coverage, and operators will recover costs at some favorable commercial rates.

We think the technology, you know, emerging technology supports very flexible mechanisms that can be configured to meet any public safety need. You can approach this from one of two ways or both ways. This is an IP based network, not a circuit switch network, which means that network operators have the ability to manage traffic in ways that protect important public safety traffic and ensure that it gets the data rates and quality of service that it needs.

Also LTE has mechanisms in the standard that use priority in determining which sessions are

established on the wireless portion of the system and which are maintained. And putting these together, we believe much can be done and the FCC will work with public safety and commercial wireless services and vendors to determine the precise needs and figure out how systems can be configured to meet them.

So Stagg talked already a lot about the cost model. You know, we had do develop a pretty detailed cost model to try and figure out how much money would be needed, and along the way I think developed a strategy which while it isn't entirely mandated is an effective blueprint for those who choose to follow it. Part of that strategy as you've already heard is to separate serving the first 95 percent where there is already a pretty good existing foot print, and the last 5 percent.

Within the first 95 percent we believe you can overlay the commercial LTE network. There is already, you know, cellular infrastructure out there that reaches 290 million Americans. Public safety can use these, these same towers, to get the coverage and signal reliability they need for a much smaller number of users. And we estimate 41,000 towers should be plenty to do that. And I'll talk a little bit more about the devices, but that's also assuming devices

that are essentially what commercial users are already using, or ruggedized versions of those.

For the remaining 5 percent we see something a little bit different, where vehicles play a larger role. So public safety again will use and harden LMR, whatever towers exist, but we also know that there will be some additional towers that may be needed, and that was figured in the cost. And to reduce the number of these towers we also imagine externally mounted antennas and perhaps repeaters placed in cars, fire trucks, police cars, that can help you get in building coverage or in the area of the incident.

So we also built into this cost model that the system would be designed to meet public safety standards, which may be more stringent, and relied on NPSTC and PSST stated requirements for things like path loss to make sure that you had the coverage you need, perhaps better than some commercial cellulars will provide, or cellular operators. And that's at least the 95 percent. For the highly rural areas, as I said, we assume the vehicular systems play a useful role as well.

And the cost model assumes these commercial technologies for mobile handsets, or variations of them. That in some ways is a conservative assumption

in that if you allow your devices to have external antennas or transmit at a higher power you could do even better, you can get better coverage, better data rates. But we made the conservative assumption, and we think the value of that can be seen by thinking about the device ecosystem. That is, there's a great opportunity to leverage LTE to get commercial economies of scale as long as you can reuse components.

And you see down here a chart with different columns for different pieces of a mobile device. The portions that would be most expensive to customize, like the RF chipset and the baseband chipset, is if you can reuse those by having similar requirements, you get to take advantage of those economies of scale and we believe you can have costs that are close to what an unsubsidized commercial device might have.

So also built into the cost model is this idea of incentive based partnerships which we think have many advantages, increased redundancy and reliability, improved capacity, reduced cost, even improved commercial infrastructure because if you put them together you improve one you can improve the other, transition path to increase spectral and operational efficiency, and this ability to use

commercial technology.

And in thinking about this, we thought of a wide range of sharing possibilities, from public safety having its own system on the left, a dedicated network, to full sharing on the right, and we came to the conclusion that a very cost effective approach was actually something in the middle, in the red box, where public safety has its own dedicated radio access network and can control that and configure that to meet its needs, but it can take advantage of commercial towers and commercial back haul wherever it can find them, and that met for a nice compromise.

And I love the figure with the antennas but I think we're behind schedule, so I'll skip it. Stagg has already talked about deployables, we imagine sort of two flavors of them, one is a cell site you can move to where it's needed, whether that's an area where the hurricane has taken out your infrastructure or you just need to supplement, and the other is these vehicular systems where particularly in highly rural areas you can move capabilities where you need them.

So summarize, I think we have a plan that ensures that broadband wireless communications for public safety will be fully interoperable across all geographies and all jurisdictions, ensures nationwide

coverage. Part of ensuring nationwide coverage is providing funding for the construction, operation, and evolution of this network. We have provide for reserve capacity and redundancy and reliability through roaming and priority access to commercial networks. And ensures that the public safety will have handsets available at reasonable consumer electronic prices. Thank you.

MR. KNAPP: Thanks, John and Stagg. Let me introduce our distinguished panelists this morning, and they're seated at the table in the right order of presentation, which happens very rarely. Allan Sadowski is the Information Technology Manager at the North Carolina State Highway Patrol. Robert LeGrande is former Chief Technology Officer of the District of Columbia Government and the President and Chief Executive Officer of LeGrande Technical and Social Services. Patrick Ringqvist is Vice President Wireless Network Solutions at Ericsson. Roger Quayle is the Chief Technology Officer and cofounder of IP Wireless.

Mark McDiarmid is the Director of RF/RAN Systems Engineering at T-Mobile. And Dale Hatfield is the Executive Director of the Silicon Flatiron Center at the University of Colorado at Boulder. And the

only panelist who has not been introduced is Walter Johnston who is sitting down there at the end who is the Chief of EMC Analysis Division in the Office of Engineering and Technology. You've already met Stagg and John. And so, Allan, if you could start with your presentation, and I am going to hold each of the presentations to ten minutes so that we can pack a lot of information in quickly, and the clock has started. Thank you.

MR. SADOWSKI: Thank you. I have to open mine up with, it's one perspective, I don't represent all public safety but I'll try to do my best. And I do have a standard disclosure that I have to do because it would take too long. I have to hit these I guess. And so it just simply says, I may be wrong and my organization will back me up until I am wrong.

(Laughter.)

MR. SADOWSKI: Okay, let it be clear that because I'm a public safety representative my focus is the mission of public safety. IT and communications is not the primary mission of public safety, it is taking care of our citizens. We respond to incidents and events in rural areas, the tribal areas, wildernesses, out there on the water, and in parks. And for my folks, that's critical that we can support